Achieving One-Round Password-Based Authenticated Key Exchange over Lattices

Zengpeng Li and Ding Wang, *Member, IEEE*

Abstract—*Password-based authenticated key exchange* (PAKE) protocol, a widely used authentication mechanism to realize secure communication, allows protocol participants to establish a high-entropy session key by pre-sharing a low-entropy password. An open challenge in PAKE is how to design a quantum-resistant round-optimal PAKE. To solve this challenge, lattice-based cryptography is a promising candidate for post-quantum cryptography. In addition, Katz and Vaikuntanathan (ASIACRYPT'09) design the first *three-round* PAKE protocol by leveraging the smooth projective hash function (SPHF) over lattices. Subsequently, Zhang and Yu (AISACRYPT'17) optimized Katz-Vaikuntanathan's approximate SPHF via a splittable public key encryption. They then constructed a *two-round* PAKE by using the simulation-sound non-interactive zero-knowledge (NIZK) proofs, but how to construct a lattice-based simulation-sound NIZK remains an open research question. In other words, how to design a one-round PAKE via an efficient lattice-based SPHF still remains a challenge. In this work, we attempt to fill this gap by proposing a lattice-based SPHF with adaptive smoothness. We then obtain a *one-round* PAKE protocol over lattices with rigorous security analysis by integrating the proposed SPHF into the one-round framework proposed by Katz and Vaikuntananthan (TCC'11). Furthermore, we explore the possibilities of achieving two-round PAKE and universal composable (UC) security from our SPHF, and show the potential application of our PAKE in Internet of Things (IoTs) where communication cost is the main consideration.

Index Terms—Password-based authenticated key exchange, smooth projective hash function, lattice-based cryptography

1 Introduction

Password-based authentication still constitutes the most widespread method of authentication [1], [2], especially on the Internet today, e.g., [3], [4]. Password-based authenticated key exchange (PAKE) protocol is an important cryptographic primitive that enables two players (e.g., a client and a server) to generate a high entropy session key by pre-sharing a common, low-entropy password. Then, the players could utilize the established session key to protect communications over an insecure network (see Fig. 1). Building on earlier literatures such as the EKE (a.k.a., encrypted key exchange) scheme [5] and the Bellare-Pointcheval-Rogaway (BPR) model [6], the classical Kata-Ostrorsky-Yung (in short KOY) framework [7] is proposed under the decisional Diffie-Hellman (DDH) assumption. Subsequently, Gennaro and Lindell (hereafter GL scheme) [8] generalized the KOY scheme by introducing the smooth projective hash function (SPHF) in the BPR security model. Since then, considerable attention [9], [10], [11], [12] has been devoted to the development of round-optimal PAKE protocols via efficient SPHFs.

The concept of SPHF was first denoted by Cramer and Shoup [13]. The authors used SPHF to gain the first encryption scheme that is indistinguishable against (adaptive) chosen ciphertext attacks (or IND-CCA2) under the DDH assumption in the standard model. A number of DDH-based or lattice-based SPHFs have been successively proposed (e.g., [9], [14], [15]). With these SPHFs as the building block, constant-round PAKE protocols (e.g., [9], [10], [12], [15]) can be obtained. However, most of these PAKE protocols are built on DDH-based SPHFs in the group (or pair) setting.

According to our investigation, most of the existing PAKE protocols (e.g., [9], [16], [17], [18]) under the GL framework [8] need at least three rounds, and they leverage IND-CCA2 encryption schemes to establish a high-entropy session key. However, how to reduce communication rounds and relax the security requirement of the underlying primitives remain two research challenges that have yet to be resolved. Notably, Jiang and Gong [16] relaxed the security of GL framework by using the combination of an IND-CPA (indistinguishable against chosen plaintext attacks) scheme at the user-side and an IND-CCA2 scheme at the server-side. However, their PAKE protocol still needs three rounds of communication. In 2015, Abdalla et al. [19] improved the GL framework and obtained a two-round PAKE protocol under the DDH-based SPHF, where the client requires an IND-CPA-secure scheme and the server requires an indistinguishable against plaintext checkable attack (IND-PCA) resistant scheme. Note that an IND-CCA2-secure scheme is equivalent to an IND-PCA-secure scheme. However, most of the aforementioned PAKE protocols (e.g., [16], [17], [18]) under the DDH assumptions are insecure in the coming quantum era.

- *Z. Li is with the College of Computer Sciences and Technology, Qingdao University, Qingdao 266071, P.R. China, and also with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, United Kingdom. E-mail: zengpengli@hotmail.com.*
- *D. Wang is with the School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China, and also with State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China. E-mail: wangdingg@pku.edu.cn.*

Manuscript received 24 Oct. 2018; revised 20 June 2019; accepted 23 Aug. 2019. Date of publication 6 Sept. 2019; date of current version 4 Feb. 2022.
(Corresponding author: Ding Wang.)
Digital Object Identifier no. 10.1109/TSC.2019.2939836